САИБ

Программа повышения осведомленности сотрудников компании

+7 (383) 255 32 55 info@saib.biz saib.biz

saib.biz
info@saib.biz
+7 (383) 255 32 55

Аннотация

Человеческий фактор - это одна из основных причин взломов компаний при помощи социальной инженерии и широковещательных вирусных атак.

Недопонимание важности включения в комплексную систему корпоративной безопасности всех структурных подразделений компании не позволяет достичь достаточного уровня эффективности системы защиты корпоративных ресурсов и внутреннего контроля.

Ликвидации этих пробелов в профессиональной подготовке сотрудников компании посвящен этот курс.

В курсе в общедоступной форме дается информация об основах поведения в информационной среде предприятия и сторонних информационных средах для снижения вероятности мошеннических действий.

Курс помогает понять, какие действия в информационной среде в Интернете и электронной почте являются нормальными, а какие могут привести к плачевным последствиям.

САИБ

Программа повышения осведомленности сотрудников компании

saib.biz
info@saib.biz
+7 (383) 255 32 55

Содержание курса

Базовые правила безопасности

Данный курс направлен на обучение базовым правилам безопасности и
умение предотвращать возникающие угрозы, находясь в офисе или за его пределами.
Вы познакомитесь с оптимальными методами работы,
которые помогут обеспечить безопасность данных, устройств, сети и рабочего места

Безопасность электронной почты

В данном курсе вы научитесь отличать поддельные письма
от оригинальных на основе некоторых характеристик, при наличии которых,
можно выявить атаку с помощью одного из методов социотехники - фишинга

Как избежать опасных вложений

Поймете для чего и зачем злоумышленники используют вложения в обманных электронных сообщениях
Научитесь определять безопасные вложения по их расширениям
Научитесь правильно обращается с неизвестными вложениями

Основы социальной инженерии

В ходе данного курса вы научитесь распознавать мошенничества
с использование социотехники (социальной инженерии),
обеспечивать собственную безопасность и помогать в этом своим коллегам по работе.

САИБ

Программа повышения осведомленности сотрудников компании

saib.biz
info@saib.biz
+7 (383) 255 32 55

Требования к паролям (парольная политика)

В ходе данного курса вы научитесь составлять надежные и безопасные пароли,
узнаете почему важно использовать второй фактор авторизации,
ознакомитесь с источниками скомпрометированных паролей, а так же с инструментами хранения и защиты паролей.

Антивирусная защита

В этом подкурсе рассматриваются основы теории компьютерных вирусов (что такое вирусы, классификация вирусов),
современные тенденции развития угроз, связанных с применением программного обеспечения,
принципы и технологии, используемые для борьбы с вредоносными программами и другими сетевыми угрозами.

Порядок работы с ресурсами Интернет

Данный подкурс объясняет как следует работать пользователю в сети Интернет
согласно требуемых условий безопасности.
Вы ознакомитесь с надежными источниками информации, интранет, а также с опасными и безопасными сайтами.

Установка программного обеспечения и подключение дополнительных устройств на рабочей станции Пользователей

В ходе данного курса вы ознакомитесь с регламентом подключения дополнительных устройств,
а так же согласованием заявок, списоком разрешенного оборудования, регистрацией новых устройств.

САИБ

Программа повышения осведомленности сотрудников компании

saib.biz
info@saib.biz
+7 (383) 255 32 55

Использование внешних (съемных) накопителей информации

В этом курсе вы ознакомитесь с принципами распространения вирусов через внешние USB-накопители и к чему приводит бесконтрольно использование USB-накопителей.

Обработка персональных данных

Формирование знаний и навыков, необходимых для организации и обеспечения безопасности персональных данных, обрабатываемых в информационных системах государственных, муниципальных органов, органов местного самоуправления и организаций различных форм собственности, физических лиц, организующих и (или) осуществляющих обработку персональных данных.

САИБ

Программа повышения осведомленности сотрудников компании

saib.biz
info@saib.biz
+7 (383) 255 32 55

Адаптация курса

Заключая с нами договор на обучение, вы можете дополнительно заказать услугу адаптации курса. **Данная услуга необходима организациям, которые используют уникальные средства защиты инфраструктуры компании.**

Наши специалисты проводят аудит инфраструктуры организации, выявляя элементы, на которых следует акцентировать внимание сотрудников при обучении. В комплексе аудита и сбора информации мы затрагиваем не только структуру информационной безопасности, но и документацию и регламенты работ, такие как персональные данные, заявки, правила работ с оборудованием.

Проходя обучение, персонал будет знакомиться непосредственно с нужным инструментарием.

На протяжении всего курса будут приведены примеры именно вашей инфраструктуры, что в будущем облегчит процесс адаптации сотрудника.

Вы будете уверены, что, пройдя обучение, сотрудник ознакомился абсолютно со всеми нюансами, на которые следует обращать внимание при работе с вашей инфраструктурой.

saib.biz
info@saib.biz
+7 (383) 255 32 55

Брендирование курса

При заключении договора вы можете заказать услугу брендирования курса.

У нас в штате имеются профессиональные дизайнеры и маркетологи, которые возьмутся за персонализацию учебного материала, согласно брендбуку вашей организации.

Профессиональный курс, выполненный в вашем фирменном стиле, повышает престиж организации.

Каждый брендированный курс вы можете приобрести в формате SCORM.
SCORM – это международный стандарт для создания электронного курса.

Почти любая система дистанционного обучения (СДО) поддерживает данный стандарт (**Blackboard**, **Moodle**, **OLAT**, **tools.hrm.ru** от WebSoft, **ShareKnowledge** от Competentum, **Mirapolis LMS**, **Webtutor**).

Материал, который вы загрузите в систему обучения, откроется с любого компьютера через любой интернет-браузер.

САИБ

Программа повышения осведомленности сотрудников компании

saib.biz
info@saib.biz
+7 (383) 255 32 55

Социальная инженерия и фишинговые рассылки

В настоящее время, имея даже самую современную и идеально настроенную систему безопасности, вы не можете гарантировать полную сохранность данных. **Слабым звеном является пользователь.** Если вы забоитесь о сохранности ваших конфиденциальных данных, то вам следует не только повышать осведомленность сотрудников, но и периодически проводить проверки бдительности.

Мы предоставляем услугу социнженерии и фишинговых рассылок.

Суть почтового фишинга в том, что цели отправляется электронное письмо, в котором содержится просьба выслать те или иные конфиденциальные данные. Мы детально прорабатываем все особенности работы организации, находим уязвимые точки, которые можем использовать для получения конфиденциальных и/или учетных данных.

За счет профессиональных дизайнеров и разработчиков мы достигаем правдоподобных результатов, начиная от электронных сообщений известных отправителей до форм авторизации различных сервисов.


САИБ